(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 039 724 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.09.2000 Bulletin 2000/39

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/12

(21) Application number: **99308625.5**

(22) Date of filing: **29.10.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.10.1998 US 182944**
19.05.1999 US 314601

(71) Applicant: **Nortel Networks Limited**
Montreal, Quebec H2Y 3Y4 (CA)

(72) Inventors:
- **Borsato, Larry**
  Ottawa, Ontario K1V 9C8 (CA)
- **Hamilton, Ian K.**
  Nepean, Ontario K2G 6C8 (CA)
- **Waters, Glenn**
  Stittsville, Ontario K2S 1B8 (CA)
- **Gaudet, Mark W.**
  Ottawa, Ontario J1Y 0S9 (CA)
- **Anderson, Rodrick**
  Carp, Ontario K0A 1L0 (CA)

(74) Representative: **Ryan, John Peter William et al**
Nortel Networks
Intellectual Property Law Group
London Road
Harlow, Essex CM17 9NA (GB)

(54) Method and apparatus providing for internet protocol address authentication

(57) A method and apparatus for storage of user identifier / IP address pairs in a network. The network includes a DHCP server for assigning IP addresses to computer and other devices in the network, a device (such as a computer) coupled to receive an IP address from the DHCP server, an authentication server coupled with the device for receiving user identifier / IP address pairs from the device and authenticating the user, and a directory server coupled to receive authenticated user identifier / IF address pairs from the authentication server.

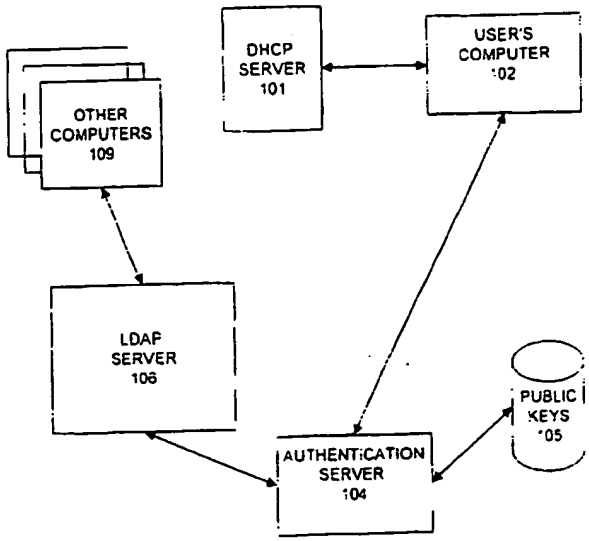

FIGURE 1

EP 1 039 724 A2

formation.

[0028] As will be appreciated, the authentication of the user id and IP address pair known to be valid only at the instant of authentication. In certain embodiments, it may be useful to provide for a time out or other mechanism which requires the user to re-authenticate after some event (such as the expiration of a period of time).

[0029] Turning briefly to **Figure 3**, a high level block diagram illustrating components of the LDAP server **106** is shown. The LDAP server **106** comprises a database of authenticated user id/IP address pairs **304**. These pairs have, in the described embodiment, been received from the authentication server **104** using a communication program **302** executed on processor **306** for receiving the user id/IP address pairs. Applications executing on requesting devices **109** may request access to the user id/IP address pairs **304** by using communication program **301**.

[0030] Certain implementations may not require security. In such implementations, aspects of the present invention may be implemented without requirement for use of the authentication techniques discussed above. Therefore, the present application may refer to the authentication server **104** simply as a binding server. The binding server and LDAP server (or other database) may be referred to collectively as a "binding system" which serves to associate a user identifier with dynamic information about the user (such as an IP address) and store the information in a data store.

[0031] Thus, what has been disclosed is a method and apparatus for authenticating users/internet protocol (IP) address pairs.

Claims

1. A method comprising:

   providing an internet protocol (IP) address to a computer;
   establishing a connection between the computer and a server;
   receiving by the server the IP address and a corresponding user identifier and to be used by a user of the computer; and
   storing the user identifier/IP address pair in a data store.

2. The method as recited by claim 1, wherein the establishing of the connection includes

   authenticating the user; and
   establishing a secure connection between the computer and the server if the user is authenticated.

3. The method as recited by claim 1, wherein the assigning of the internet protocol address includes

   initiating a request by the computer to a dynamic host configuration protocol (DHCP) server; and
   assigning the IP address by the DHCP server; and
   sending the IP address to the computer.

4. The method as recited by claim 1, wherein the data store includes a database of a Lightweight Directory Access Protocol server.

5. A server comprising:

   a first data store having stored therein an authenticated user identifier / internet protocol address pair; and
   a second data store having stored therein a program which when executed on a processor retrieves the authenticated user identifier / internet protocol address pair and transmits the pair to a requesting device.

6. The server as recited by claim 5, further comprising:
   a third data store having stored therein a program which when executed on a processor stores authenticated user identifier / internet protocol address pairs received from an authentication server.

7. A method comprising:

   a first device communicating with a dynamic host configuration protocol (DHCP) server to have an internet protocol (IP) address assigned to the first device;
   the first device communicating with an authentication server a user identifier and the IP address;
   the authentication server authenticating the user;
   the authentication server communicating to a lightweight directory access protocol (LDAP) server the user identifier / IP address pair; and
   the LDAP server storing the user identifier / IP address pair.

8. A network comprising:

   a dynamic host configuration protocol (DHCP) server;
   a computer coupled in communication with the DHCP server over the network to receive an internet protocol (IP) address;
   an authentication server coupled in communication over the network with the computer, the authentication server to authenticate a user using the computer based on a user identifier communicated from the computer; and
   a directory server coupled in communication

with the authentication server, the directory server to receive and store both the authenticated user identifier and its corresponding IP address from the authentication server.

9. The network as recited by claim 8, wherein the directory server is a lightweight directory access protocol (LDAP) server.

10. The network as recited by claim 8 further comprising requesting devices coupled in communication with the directory server for requesting authenticated user identifier / IP address pairs.

11. A network comprising a DHCP server for assigning internet protocol (IP) addresses to computer and other devices in the network, a device coupled to receive an IP address from the DHCP server, an authentication server coupled with the device for receiving user identifier / IP address pairs from the device and authenticating the user, and a directory server coupled to receive authenticated user identifier / IP address pairs from the authentication server.

12. A lightweight directory access protocol (LDAP) server comprising:

a first data store having stored therein an user identifier / internet protocol address pair; and
a second data store having stored therein a program which when executed on processor retrieves the user identifier / internet protocol address pair and transmits the pair to a requesting device.

13. A lightweight directory access protocol (LDAP) server comprising:

a first data store having stored therein an user identifier and dynamic information related to the user identifier; and
a second data store having stored therein a program which when executed on processor retrieves the user identifier and dynamic information and transmits the information to a requesting device.

14. The LDAP server as recited by claim 13, further comprising a third data store having stored therein a program which when executed on a processor stores dynamic information related to a user identifier in the first data store.

15. The LDAP server as recited by claim 14, wherein the dynamic information is an internet protocol address.

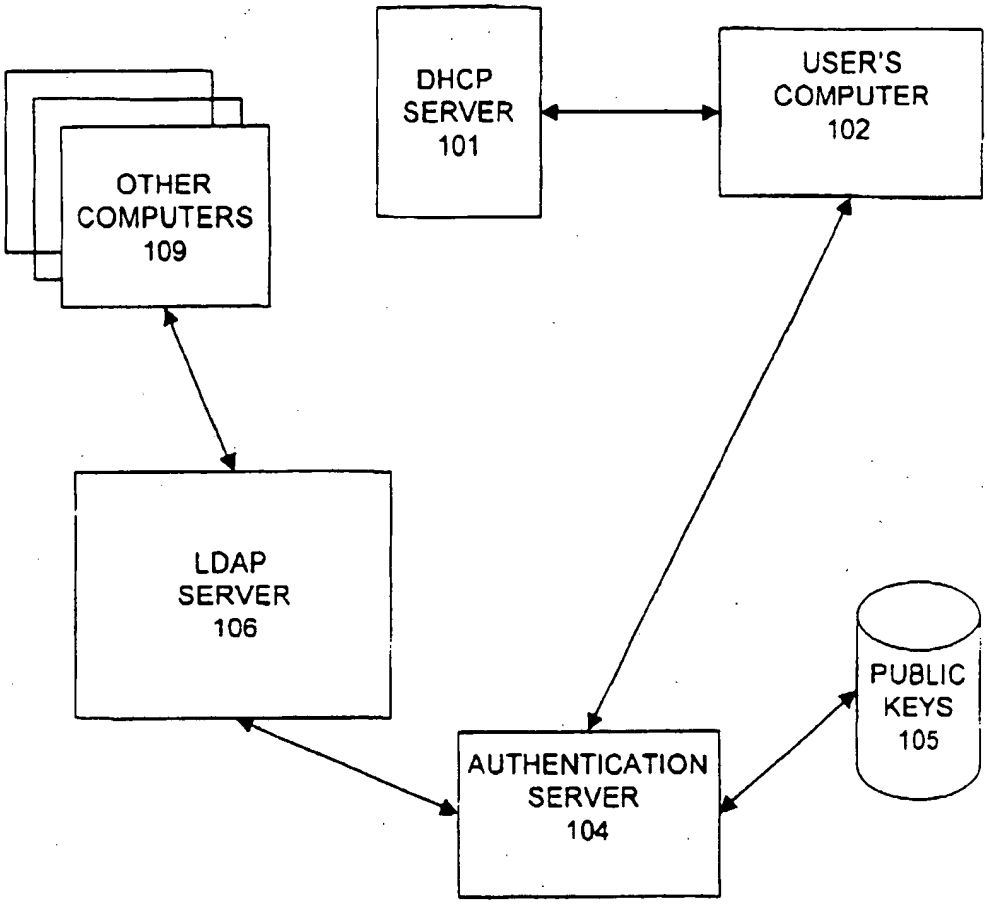

FIGURE 1

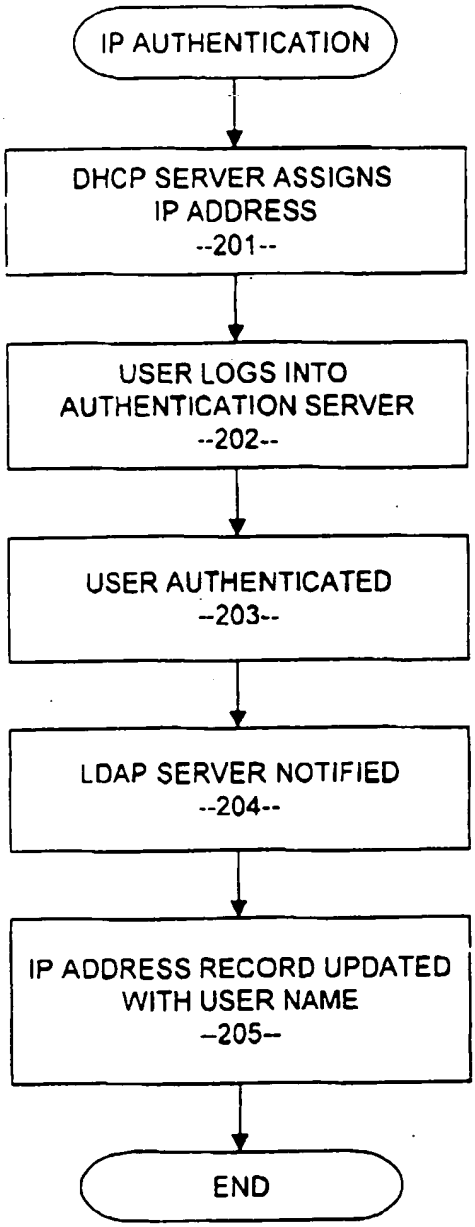
IP AUTHENTICATION
DHCP SERVER ASSIGNS IP ADDRESS --201--
USER LOGS INTO AUTHENTICATION SERVER --202--
USER AUTHENTICATED --203--
LDAP SERVER NOTIFIED --204--
IP ADDRESS RECORD UPDATED WITH USER NAME --205--
END

FIGURE 2

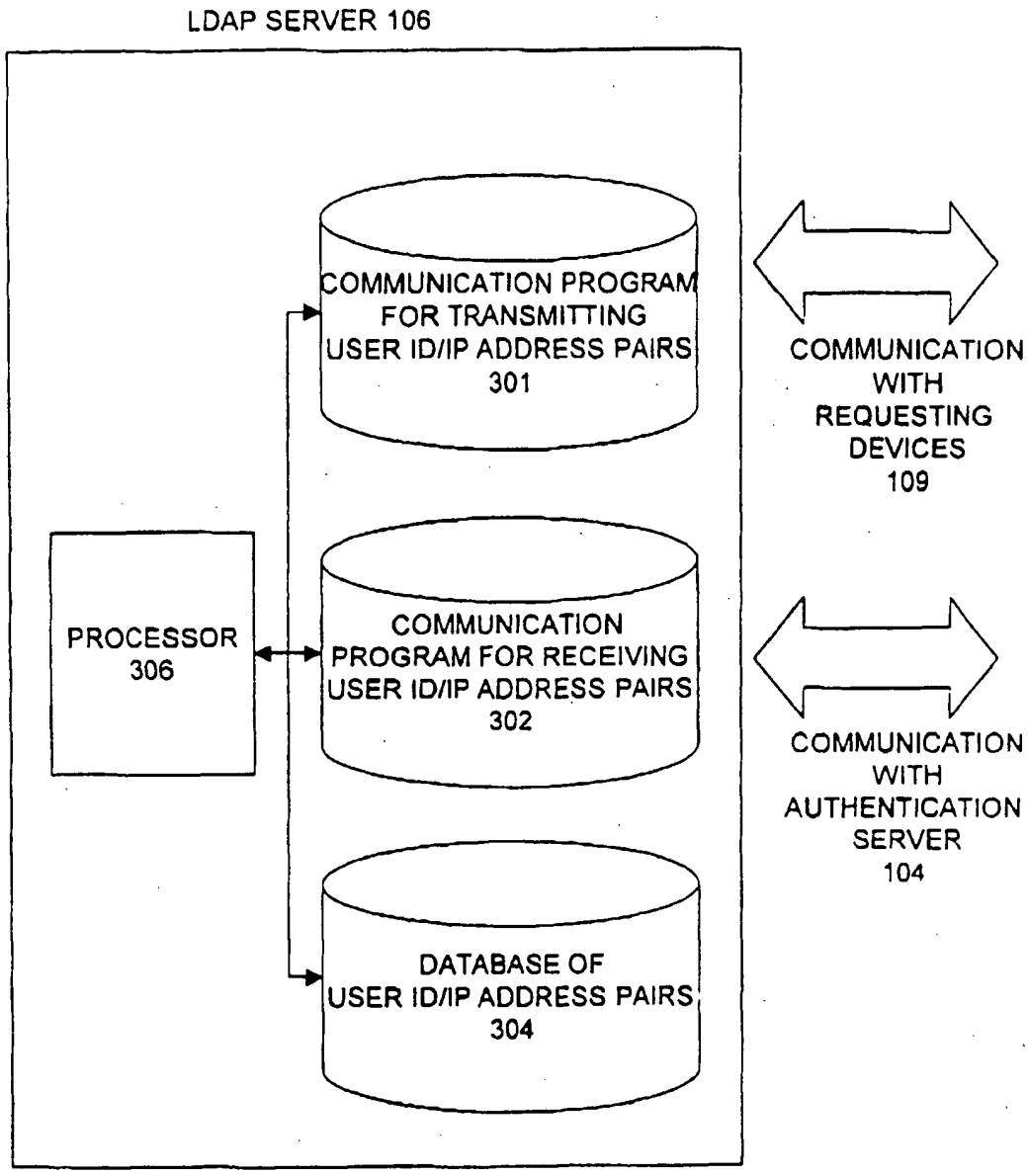

FIGURE 3